UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/991,932	11/26/2001	Akiko Miyagawa	2565-0238P	9870

2292 7590 06/20/2006

BIRCH STEWART KOLASCH & BIRCH
PO BOX 747
FALLS CHURCH, VA 22040-0747

EXAMINER	
NOBAHAR, ABDULHAKIM	
ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 06/20/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/991,932	MIYAGAWA ET AL.	
	Examiner	Art Unit	
	Abdulhakim Nobahar	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *26 May 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-17* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-5,7-13 and 17* is/are rejected.

7)☒ Claim(s) *6 and 14-16* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This communication is in response to applicants' response received on May 26, 2005.

2. Amendments of claims 1, 3, 9 and 13 are acknowledged.

3. Applicants' arguments with respect to the rejections of claims 1-5, 7-13 and 17 under 35 USC § 112, 102 and 103 have been fully considered and are persuasive. Therefore, the rejections have been withdrawn. However, upon further consideration of the amended claims, a new ground(s) of rejection is made.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-5, 7-13 and 17 are rejected under 35 U.S.C. 102(e) as being unpatentable over Rothermel et al (6,678,827 B1; hereinafter Rothermel) in view of Osborne et al (6,687,833 B1; hereinafter Osborne).

Claims 1 and 9

Rothermel discloses:

A control system (see col. 1, lines 22-36; col. 5, lines 14-25; col. 14, lines 50-59); and

an illegal access data handling apparatus, placed outside a given internal communication network (see col. 1, lines 22-36, where unauthorized external access corresponds to the recited illegal access data; col. 6, lines 7-20, where the Network Security Device Management and the supervisor devices are functionally equivalent to the recited illegal access data handling apparatus; col. 14, lines 50-59), for receiving illegal access data transmitted from a data communication device placed outside the internal communication network for a purpose of illegally accessing the internal communication network (see col. 6, lines 7-20; col. 9, lines 14-27, where an NSD transmits security information about an event of interest corresponding to the recited illegal access data to a supervisor device), and for taking countermeasures against the illegal access data received (see col. 15, lines 30-57).

Rothermel, however, does not disclose the use of a decoy server and providing a response pretending to originate from the internal communication network.

Osborne, on the other hand teaches a system and a method deploying a network host decoy to protect a network against attack by illicit users (see abstract and col. 1, lines 38-49). Osborne further teaches that a deceptive response is sent to an attacker by a pseudo host to cause an illusion so that it appears as a real answer originating from a device at the protected network (see, for example, col. 4, lines 8-25).

It would have been obvious to a person of ordinary skill in the at the time the invention was made to deploy a decoy device as taught in Osborne in the system of

Rothermel because it provide a mechanism for better deception and more convincing and realistic to a would-be attacker (Osborne, col. 2, lines 52-55).

Claim 2

Rothermel discloses:

The illegal access data handling apparatus of claim 1, wherein the illegal access data handling apparatus is connected to an illegal access data detection device for relaying a data communication between a data communication device placed within the internal communication network and a data communication device placed outside the internal communication network (see col. 4, lines 30-48; col. 6, lines 7-20, where the Network Security Device Management and the supervisor devices are functionally equivalent to the recited illegal access data handling apparatus and the Network Security Device that is placed between external devices and the internal devices corresponds to the recited illegal access data detection device), and for detecting the illegal access data, and wherein the illegal access data handling apparatus receives the illegal access data from the illegal access data detection device (see col. 15, lines 3-15; col. 16, lines 7-55, where the NSD detects unauthorized packets and transmits information related to this event to a supervisor device).

Claim 3

Rothermel discloses:

The illegal access data handling apparatus of claim 2, comprising:

a data reception section for receiving the illegal access data from the illegal access data detection device (see col. 16, lines15-20);

a data analysis section for analyzing the illegal access data received by the data reception section (see col. 3, lines 45-57; col. 4, lines 43-48);

a response data generation section for generating response data to the illegal access data based upon an analysis result from the data analysis section (see col. 4, line 49-col. 5, line 13, where the templates corresponds to the recited response data); and

a data transmission section for transmitting the response data generated by the response data generation section to the illegal access data detection device (see col. 4, lines 65-col. 5, line 3).

Claim 4

Rothermel discloses:

The illegal access data handling apparatus of claim 3, wherein the data reception section receives an illegal access data from the illegal access data detection device (see col. 5, lines 55-61; col. 16, lines 15-20), and wherein the data transmission section transmits the response data to the illegal access data detection device (see col. 5, lines 55-61; col. 16, lines 15-20; col. 17, lines 23-43)

Rothermel does not expressly discloses that the illegal access data handling apparatus includes a capsulation section for decapsulating the encapsulated illegal access data received by the data reception section to extract the illegal access data, and encapsulates the response data.

Osborne, however, discloses a system for protecting an internal network from attacks originated from entities located in an external network (see Fig. 1; col. 1, lines 37-49). Osborne further discloses a capsulation mechanism deployed in the security components that encapsulate a response to an attacker before transmission (see col. 2, lines 28-51; col. 5, lines 1-11; col. 6, lines 53-67). Therefore, it would be obvious to a person of ordinary skill in the art at the time the invention was made to implement a capsulation mechanism as taught in Osborne in the system of Rothermel, because it would enable the security components of the protected system to decapsulate the receiving recursively encapsulated frames and encapsulate the response to an attacker (see Osborne, col. 2, lines 32-50).

Claim 7

Rothermel discloses:

The illegal access data handling apparatus of claim 4, wherein the data reception section receives the illegal access data having authentication information attached to be used for data authentication from the illegal access data detection device, and wherein the capsulation section performs the data authentication for the illegal access data by using the authentication information (see col. 6, lines 1-6; col. 11; lines 34-45).

Claim 8

Rothermel discloses:

The illegal access data handling apparatus of claim 7, wherein the capsulation section attaches the authentication information to be used for the data authentication for the response data to the response data, and wherein the data transmission section transmits the response data having the authentication information attached by the capsulation section to the illegal access data detection device (see col. 5, line 52-col. 6, line 6; col. 11, lines 34-45, where the communication between the NSDs and supervisor devices are encrypted and authenticated for the purpose of security and thus, the information transmitted between these devices must have required data to perform authentication process).

Claim 10

Rothermel discloses:

The method of claim 9, comprising:

communicating with an illegal access data detection device for relaying a data communication between a data communication device placed within the internal communication network and a data communication device placed outside the internal communication network, and for detecting the illegal access data (see col. 4, lines 30-48; col. 6, lines 7-20, where the Network Security Device Management and the supervisor devices are functionally equivalent to the recited illegal access data handling apparatus and the Network Security Device that is placed between external devices and the internal devices corresponds to the recited illegal access data detection device); and receiving the illegal access data from the illegal access data detection device (see col.

15, lines 3-15; col. 16, lines 7-55, where the NSD detects unauthorized packets and transmits information related to this event to a supervisor device).

Claim 11

Rothermel discloses:

The method of claim 10, comprising:

receiving the illegal access data from the illegal access data detection device (see col. 16, lines15-20);

analyzing the illegal access data received by the receiving (see col. 3, lines 45-57; col. 4, lines 43-48);

generating response data to the illegal access data based upon an analysis result from the analyzing (see col. 4, line 49-col. 5, line 13, where the templates corresponds to the recited response data); and

transmitting the response data generated by the generating to the illegal access data detection device (see col. 4, lines 65-col. 5, line 3).

Claims 13 and 17

Rothermel discloses:

receiving an unauthorized access packet at a data center placed outside the internal network, and wherein the unauthorized access packet is redirected from a target server residing within the internal network (see col. 6, lines 7-20; col. 9, lines 14-27; col. 16, lines15-20);

analyzing the received packet to formulate a response packet (see col. 3, lines 45-57; col. 4, lines 43-48);

sending the response packet to the network device, wherein the network device is within the internal network (see col. 4, lines 65-col. 5, line 3, where the templates corresponds to the recited response data).

Rothermel does not expressly discloses that the illegal access data handling apparatus includes a capsulation section for decapsulating the encapsulated illegal access data received by the data reception section to extract the illegal access data, and encapsulates the response data.

Osborne, however, discloses a system for protecting an internal network from attacks originated from entities located in an external network (see Fig. 1; col. 1, lines 37-49). Osborne further discloses a capsulation mechanism deployed in the security components that encapsulate a response to an attacker before transmission (see col. 2, lines 28-51; col. 5, lines 1-11; col. 6, lines 53-67). Therefore, it would be obvious to a person of ordinary skill in the art at the time the invention was made to implement a capsulation mechanism as taught in Osborne in the system of Rothermel, because it would enable the security components of the protected system to decapsulate the receiving recursively encapsulated frames and encapsulate the response to an attacker (see Osborne, col. 2, lines 32-50).

Regarding claims 5 and 12, Rothermel does not discloses a decoy device to respond to an illegal access attempt by an unauthorized user (e.g. a hacker) with a response to have similar content as a true response.

Osborne teaches a system and a method deploying a network host decoy to protect a network against attack by illicit users (see abstract and col. 1, lines 38-49). Osborne further teaches that a deceptive response is sent to an attacker by a pseudo host to cause an illusion so that it appears as a real answer originating from a device at the protected network (see, for example, col. 4, lines 8-25).

It would have been obvious to a person of ordinary skill in the at the time the invention was made to deploy a decoy device as taught in Osborne in the system of Rothermel because it provide a mechanism for better deception and more convincing and realistic to a would-be attacker (Osborne, col. 2, lines 52-55).

Allowable Subject Matter

Claims 6 and 14-16 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

US Patent No 6,880,090 B1 to Shawcross.

US Patent Application Pub. No 2004/0117478 A1 to Triulzi et al.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Abdulhakim Nobahar whose telephone number is 571-272-3808. The examiner can normally be reached on M-T 8-6.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Abdulhakim Nobahar
Examiner
Art Unit 2132 A.N.

June 15, 2006

GILBERTO BARRON Jr.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100